اجرای ثابت‌افزار روی QEMU

با توجه به پشتیبانی شبیه‌ساز QEMU از اکثر SoC های موجود در بازار، گمان می‌رفت که SoC مربوط به Firmware پهپاد mavic 2 (یعنی allwinner H6 برای خود پهپاد و rockchip rk3066 برای کنترلر) نیز در این شبیه‌ساز وجود داشته باشد. اما با بررسی دقیق‌تر، متوجه شدیم که چنین قابلیتی وجود ندارد. آزمایش و خطای SoC های دیگر برای اجرای ثابت‌افزار، نتیجه خاصی نداشت. همچنین احتمال ناقص بودن فایل‌های ثابت‌افزار نیز وجود دارد. برای همین، به بررسی دقیق‌تر دایرکتوری‌ها و فایل‌های موجود در ثابت‌افزار می‌پردازیم.

بررسی فایل‌ها و دایرکتوری‌های ثابت‌افزار پهپاد

نکته قابل‌ذکر در مورد ثابت‌افزار پهپاد، این است که فایل قرار داده‌شده در سایت مرجع، دارای دو فولدر ۰۸۰۱ و ۰۹۰۱ می‌باشد. فولدر ۰۹۰۱ مربوط به leadcore SOC می‌باشد و طبق گفته سایت، ارزش تحلیل را ندارد. اما فولدر ۰۸۰۱ مربوط به Allwinner SoC می‌باشد و به‌طور کلی می‌توان گفت که ثابت‌افزار هدف ما برای بررسی است. در این بخش به بررسی فایل‌ها و دایرکتوری‌های مربوط به ۰۸۰۱ می‌پردازیم.

- فایل build.prop در ۰۸۰۱
  - یک فایل سیستمی که شامل مشخصات build و تنظیمات سیستم اندروید می‌باشد.
  - برخی از محتوا این فایل بسته به سازنده متفاوت است.
  - با اعمال تغییرات می توان برخی از تنظیمات غیرقابل دسترسی اندروید را تغییر داد.

build.prop
~/Hardware_Lab/FirmWare/mavic2_dump/0801

```
ro.product.device=eagle_wm240
ro.product.board=evb2
# ro.product.cpu.abi and ro.product.cpu.abi2 are obsolete,
# use ro.product.cpu.abilist instead.
ro.product.cpu.abi=armeabi-v7a
ro.product.cpu.abi2=armeabi
ro.product.cpu.abilist=armeabi-v7a,armeabi
ro.product.cpu.abilist32=armeabi-v7a,armeabi
ro.product.cpu.abilist64=
ro.product.manufacturer=DJI
ro.product.locale=en-US
ro.wifi.channels=
ro.board.platform=eagle
# ro.build.product is obsolete; use ro.product.device
ro.build.product=eagle_wm240
# Do not try to parse description, fingerprint, or thumbprint
ro.build.description=full_eagle_wm240-userdebug 6.0 MDB08M 94 test-keys
ro.build.fingerprint=eagle/full_eagle_wm240/eagle_wm240:6.0/MDB08M/94:userdebug/test-keys
ro.build.characteristics=default
# end build properties

#
# ADDITIONAL_BUILD_PROPERTIES
#
dji.build.version=10.00.06.35
persist.sys.dalvik.vm.lib.2=libart
dalvik.vm.isa.arm.variant=cortex-a7
dalvik.vm.isa.arm.features=default
dalvik.vm.lockprof.threshold=500
```

- فایل recovery-from-boot.p

- دایرکتوری lost+found
  - فولدری که در آن فایل‌های گم شده یا حذف شده نگهداری می شود.
  - مختص لینوکس و UNIX
- دایرکتوری bin
  - فولدری که در آن فایل های باینری قرار دارد.
  - همه فایل های قابل اجرا os مانند ls و cat و ... در این فولدر قرار دارند.
  - دایرکتوری دیگری در این فولدر وجود ندارد.
- دایرکتوری lib
  - شامل کتابخانه های نصب شده روی سیستم عامل می باشد.
    ماژول های کرنل نیز در این دایرکتوری قرار دارند.
- دایرکتوری etc
  - شامل directory configuration های لینوکس
  - در فولدر ۰۸۰۱/etc تعدادی از کانفیگ مرتبط به خود پهپاد و اجزای آن مانند دوربین قرار دارند.
- دایرکتوری usr
- دایرکتوری xbin
  - اطلاعات خاصی در مورد این دایرکتوری وجود ندارد اما تنها نکته ای که در باره این دایرکتوری می‌دانیم این است که این دایرکتوری در اندرویدهای نسخه ۶ و ۷ وجود داشته است.

با مقایسه دایرکتوری‌ها و فایل‌های ذکر شده، متوجه می‌شویم که ساختار File System این ثابت‌افزار نه به طور کامل اندروید و نه لینوکس می باشد و یک چیزی بین این دو File System است.